Serial No. 09/884,672
Art Unit No. 2134

LISTING OF CLAIMS

1.   (currently amended)   An ad-hoc radio communication verification system, comprising:

means for sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the one data send/receive device, means for generating verification data from the sent data for verification data generation produced using based on a first generation algorithm and outputting the generated verification data to its own verification data output section;

in the other data send/receive device, means for generating verification data from the received data for verification data generation produced using based on the first generation algorithm and outputting the generated verification data to its own verification data output section; and

means for determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually,

JP920000134US1   -3-

Serial No. 09/884,672
Art Unit No. 2134

wherein the first generation algorithm generates a
plurality of verification data, wherein for each
verification data, it is determined whether the verification
data at the verification data output sections of both the
data send/receive devices match mutually.

2. (original) The ad-hoc radio communication verification
system according to claim 1, wherein the verification data
is visual or auditory verification data.

3. (original) The ad-hoc radio communication verification
system according to claim 1, wherein the verification data
is output at the verification data output section both in
the visual form and auditory form.

4. (currently amended) The ad-hoc radio communication
verification system according to claim 1, further
comprising:

means for defining a function as an operator, for
defining a numeric on which the operator operates as an
input to of the operator, and for defining an operation
result of the operator as an output of the operator;

JP920000134US1   -4-

Serial No. 09/884,672
Art Unit No. 2134

means for establishing a serial sequence of operators that are composed of <u>more than</u> one <s>or more of</s> operators arranged in series, wherein the operators relate to the same or different one-way functions; and

means for letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

5. (canceled)

6. (currently amended) The ad-hoc radio communication verification system according to <u>claim 1</u> <s>claim 5</s>, further comprising:

means for defining a function as an operator, <u>for defining</u> a numeric on which the operator operates as an input <u>to</u> <s>of</s> the operator, and <u>for defining</u> an operation result of the operator as an output of the operator;

means for establishing a serial sequence of operators that are composed of two or more of operators arranged in series, wherein the operators relate to the same or different one-way functions;

JP920000134US1   -5-

Serial No. 09/884,672
Art Unit No. 2134

means for letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or corresponding values be the verification data respectively; and

means for determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

7.   (currently amended) The ad-hoc radio communication verification system according to <u>claim 1</u> <s>claim 5</s>, further comprising:

means for defining a function as an operator, <u>for defining</u> a numeric on which the operator operates as an input <u>for</u> <s>of</s> the operator, and <u>for defining</u> an operation result of the operator as an output of the operator;

means for establishing a plurality of operators that relate to mutually different one-way functions;

means for letting the data for verification data generation be a common input to each operator and an output

JP920000134US1   -6-

Serial No. 09/884,672
Art Unit No. 2134

of each operator or a corresponding value be the verification data respectively; and

means for determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

8. (original) The ad-hoc radio communication verification system according to claim 1, wherein the data for verification data generation is a public key of either data send/receive device.

9. (currently amended) An ad-hoc radio communication data send/receive system utilizing the ad-hoc radio communication verification system according to claim 8, comprising:

for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein each portable terminal comprises transmission means whereby when the ad-hoc radio communication verification system verifies that a public key Kp of one user is

JP920000134US1   -7-

Serial No. 09/884,672
Art Unit No. 2134

transmitted from the portable terminal of the one user to

the portable terminal of the other user without being

tampered with, as determined by the ad-hoc radio

communication system, and the public key Kp is transmitted

from the portable terminal to the personal computer of each

user, and wherein each personal computer comprises means to

generate a symmetric key Kc such that then the personal

computer of the other user generates a symmetric key Kc

produced using based on a second generation algorithm, while

the personal computer of the one user generates the

symmetric key Kc produced using based on the second

generation algorithm from information including a random

number and an identifier for the second generation algorithm

transmitted from the personal computer of the other user in

cipher using according to the public key; and thereafter

both the personal computers send and receive data in cipher

using according to the symmetric key Kc.

10. (currently amended) An ad-hoc radio communication data

send/receive system utilizing the ad-hoc radio communication

verification system according to claim 8, comprising, for

each user, a portable terminal having a radio communication

function   and   a   personal   computer   having   a   radio

JP920000134US1   -8-

Serial No. 09/884,672
Art Unit No. 2134

communication function that are owned by each user, wherein

the portable terminal and personal computer of each user are

connected by a secure communication path; when the ad-hoc

radio communication verification system verifies that a

public key Kp of one user is transmitted from the portable

terminal of the one user to the portable terminal of the

other user without being tampered with, and wherein each

personal computer comprises means to generate a symmetric

key Kc such that the portable terminal of the other user

generates a symmetric key Kc produced using based on a

second generation algorithm, while the portable terminal of

the one user generates the symmetric key Kc produced using

based on the second generation algorithm from information

transmitted from the portable terminal of the other user in

cipher according to the public key, then the symmetric key

Kc is transmitted from the portable terminal to the personal

computer of each user; and thereafter both the personal

computers send and receive data in cipher using according to

the symmetric key Kc.

JP920000134US1   -9-

Serial No. 09/884,672
Art Unit No. 2134

11. (currently amended) An ad-hoc radio communication data send/receive system, comprising, for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the public key Kp is transmitted from the portable terminal to the personal computer of each user, and wherein each personal computer comprises means to generate a symmetric key Kc such that ~~then~~ the personal computer of the other user generates a symmetric key Kc produced using ~~based on~~ a second generation algorithm, while the personal computer of the one user generates the symmetric key Kc produced using ~~based on~~ the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the

JP920000134US1   -10-

Serial No. 09/884,672
Art Unit No. 2134

personal computers send and receive data in cipher using according to the symmetric key Kc.

12. (currently amended) An ad-hoc radio communication data send/receive system, comprising, for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, and wherein each personal computer comprises means to generate a symmetric key Kc such that the portable terminal of the other user generates a symmetric key Kc produced using based on a second generation algorithm, while the portable terminal of the one user generates the symmetric key Kc produced using based on the second generation algorithm from information transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key Kc is transmitted from the portable terminal to the personal computer of each user; thereafter both the personal

JP920000134US1   -11-

Serial No. 09/884,672
Art Unit No. 2134

computers send and receive data in cipher using ~~according to~~ the symmetric key Kc.

13. (currently amended) A method for verifying an ad-hoc radio communication, comprising the steps of:

sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the one data send/receive device, generating verification data from the sent data for verification data generation produced using ~~based on~~ a first generation algorithm and outputting the generated verification data to its own verification data output section;

in the other data send/receive device, generating verification data from the received data for verification data generation produced using ~~based on~~ the first generation algorithm and outputting the generated verification data to its own verification data output section; and

determining whether the verification data at the sections of both the data sections of both the data send/receive devices matches mutually.

JP920000134US1   -12-

Serial No. 09/884,672
Art Unit No. 2134

<u>wherein the first generation algorithm generates a</u>
<u>plurality of verification data, wherein for each</u>
<u>verification data, it is determined whether the verification</u>
<u>data at the verification data output sections of both the</u>
<u>data send/receive devices match mutually</u>.

14. (original) The method according to claim 13, wherein the
verification data is visual or auditory verification data.

15. (original) The method according to claim 13, wherein the
verification data is output at the verification data output
section both in the visual form and auditory form.

16. (currently amended) The method according to claim 13,
further comprising the steps of:

defining a function as an operator, <u>defining</u> a numeric
on which the operator operates as an input <u>to</u> ~~of~~ the
operator, and <u>defining</u> an operation result of the operator
as an output of the operator;

establishing a serial sequence of operators that are
composed of <u>more than</u> one ~~or more of~~ operators arranged in
series, wherein the operators relate to the same or
different one-way functions;

JP920000134US1   -13-

Serial No. 09/884,672
Art Unit No. 2134

letting an input to the serial sequence of operators
be the data for verification data generation and an output
from the serial sequence of operators or a corresponding
value be the verification data.

17. (canceled)

18.   (currently amended) The method according to <u>claim 13</u>
<s>claim 17</s>, further comprising the steps of:

defining a function as an operator, <u>defining</u> a numeric
on which the operator operates as an input <u>to</u> <s>of</s> the
operator and <u>defining</u> an operation result of the operator as
an output of the operator;

establishing a serial sequence of operators that are
composed of two or more of operators arranged in series
wherein the operators relate to the same or different
one-way functions;

letting an input to the serial sequence of operators
be the data for verification data generation and outputs of
two or more of operators selected from all operators
composing the serial sequence of operators or corresponding
values be the verification data respectively; and

determining for each verification data whether the

JP920000134US1   -14-

Serial No. 09/884,672
Art Unit No. 2134

verification data match mutually at the verification data

output sections of both the data send/receive devices.

19. (currently amended) The method according to <u>claim 13</u>

~~claim 17~~, further comprising the steps of:

defining a function as an operator, <u>defining</u> a numeric

on which the operator operates as an input <u>to</u> ~~of~~ the

operator, and <u>defining</u> an operation result of the operator

as an output of the operator;

establishing a plurality of operators that relate to

mutually different one-way functions;

letting the data for verification data generation be a

common input to each operator and an output of each operator

or a corresponding value be the verification data

respectively; and

determining for each verification data whether the

verification data match mutually at the verification data

output sections of both the data send/receive devices.

20. (original) The method according to claim 13, wherein

the data for verification data generation is a public key of

either data send/receive device.

JP920000134US1   -15-

Serial No. 09/884,672
Art Unit No. 2134

21. (currently amended) The method for sending and receiving ad-hoc radio communication data, utilizing the verification method according to claim 20, comprising: a portable terminal having a radio communication function for each user and a personal computer having a radio communication function for ~~that are owned~~ by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the verification method verifies that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the public key Kp is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key Kc produced using ~~based on~~ a second generation algorithm, while the personal computer of the one user generates the symmetric key Kc produced using ~~based on~~ the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the personal computers send and receive data in cipher using ~~according to~~ the symmetric key Kc.

JP920000134US1   -16-

Serial No. 09/884,672
Art Unit No. 2134

22. (currently amended) The method for sending and-receiving ad-hoc radio communication data, utilizing the verification method according to claim 20, comprising: a portable terminal having a radio communication function <u>for each user</u> and a personal computer having a radio communication function <u>for</u> ~~that are owned by~~ each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the verification method verifies that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the portable terminal of the other user generates a symmetric key Kc <u>produced using</u> ~~based on~~ a second generation algorithm, while the portable terminal of the one user generates the symmetric key Kc <u>produced using</u> ~~based on~~ the second generation algorithm from information transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key Kc is transmitted from the portable terminal to the personal computer of each user; and thereafter both the personal computers send and receive data in cipher <u>using</u> ~~according to~~ the symmetric key Kc.

JP920000134US1   -17-

Serial No. 09/884,672
Art Unit No. 2134

23. (currently amended) The method for sending and receiving ad-hoc radio communication data, comprising: a portable terminal having a radio communication function for each user and a personal computer having a radio communication function for ~~that are owned by~~ each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the public key Kp is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key Kc produced using ~~based on~~ a second generation algorithm, while the personal computer of the one user generates the symmetric key Kc produced using ~~based on~~ the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the personal computers send and receive data, in cipher using ~~according to~~ the symmetric key Kc.

JP920000134US1   -18-

24. (currently amended) The method for sending and receiving ad-hoc radio communication data, comprising: a portable terminal having a radio communication function <u>for each user</u> and a personal computer having a radio communication function <u>for</u> ~~that are owned by~~ each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the portable terminal of the other user generates a symmetric key Kc <u>produced using</u> ~~based on~~ a second generation algorithm, while the portable terminal of the one user generates the symmetric key Kc <u>produced using</u> ~~based on~~ the second generation algorithm from information transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key Kc is transmitted from the portable terminal to the personal computer of each user; thereafter both the personal computers send and receive data in cipher <u>using</u> ~~according to~~ the symmetric key Kc.

Serial No. 09/884,672
Art Unit No. 2134

25. (currently amended) A recording medium recording a
program for an ad-hoc radio communication verification
system, wherein the verification system comprising:

means for sending data for verification data generation
from one data send/receive device to the other send/receive
device, wherein the two send/receive devices are mutually
connected by an ad-hoc radio connection;

in the one data send/receive device, means for
generating verification data from the sent data for
verification data generation produced using ~~based on~~ a first
generation algorithm and outputting the generated
verification data to its own verification data output
section;

in the other data send/receive device, means for
generating verification data from the received data for
verification data generation produced using ~~based on~~ the
first generation algorithm and outputting the generated
verification data to its own verification data output
section; and

means for determining whether the verification data at
the verification data output sections of both the data
send/receive devices matches mutually.

JP920000134US1   -20-

Serial No. 09/884,672
Art Unit No. 2134

<u>wherein the first generation algorithm generates a</u>
<u>plurality of verification data, wherein for each</u>
<u>verification data, it is determined whether the verification</u>
<u>data at the verification data output sections of both the</u>
<u>data send/receive devices match mutually</u>.

26. (original) The recording medium according to claim 25,
wherein the verification data is visual or auditory
verification data.

27. (original) The recording medium according to claim 25,
wherein the verification data is output at the verification
data output section both in the visual form and auditory
form.

28. (currently amended) The recording medium according to
claim 25, wherein the verification system further
comprising:

   means for defining a function as an operator, <u>for</u>
<u>defining</u> a numeric on which the operator operates as an
input <u>to</u> ~~of~~ the operator, and <u>for defining</u> an operation
result of the operator as an output of the operator;

JP920000134US1   -21-

Serial No. 09/884,672
Art Unit No. 2134

means for establishing a serial sequence of operators that are composed of <u>more than</u> one ~~or more of~~ operators arranged in series, wherein the operators relate to the same or different one-way functions; and

means for letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

29.   (canceled)

30. (currently amended) A delivery system for delivering a program for an ad-hoc radio communication system, the verification system comprising:

means for sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the one data send/receive device, means for generating verification data from the sent data for verification data generation <u>produced using</u> ~~based on~~ a first generation algorithm and outputting the generated

JP920000134US1   -22-

Serial No. 09/884,672
Art Unit No. 2134

verification data to its own verification data output
section;

in the other data send/receive device, means for
generating verification data from the received data for
verification data generation ~~produced using~~ based on the
first generation algorithm and outputting the generated
verification data to its own verification data output
section; and

means for determining whether the verification data at
the verification data output sections of both the data
send/receive devices matches mutually,

wherein the first generation algorithm generates a
plurality of verification data, wherein for each
verification data, it is determined whether the verification
data at the verification data output sections of both the
data send/receive devices match mutually.

31.   (currently amended) A computer program product
comprising a computer usable medium having computer readable
program code means embodied therein for causing ad-hoc radio
communication, the computer readable program code means in
said computer program product comprising computer readable

JP920000134US1   -23-

Serial No. 09/884,672
Art Unit No. 2134

program code means for causing a computer to effect ~~the~~ the

functions of claim 1.

32. (currently amended) ~~31.~~ A computer program product
comprising a computer usable medium having computer readable
program code means embodied therein for causing ad-hoc radio
communication, the computer readable program code means in
said computer program product comprising computer readable
program code means for causing a computer to effect ~~the~~ the
functions of claim 4 ~~1~~.

33. (currently amended) A computer program product
comprising a computer usable medium having computer readable
program code means embodied therein for causing ad-hoc radio
communication, the computer readable program code means in
said computer program product comprising computer readable
program code means for causing a computer to effect the ~~the~~
functions of claim 9.

34. (currently amended) A computer program product
comprising a computer usable medium having computer readable
program code means embodied therein for causing ad-hoc radio
communication, the computer readable program code means in

JP920000134US1   **-24-**

Serial No. 09/884,672
Art Unit No. 2134

said computer program product comprising computer readable program code means for causing a computer to effect the ~~the~~ functions of claim 10.

35.   (original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 11.

36. (canceled)

37.   (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13.

JP920000134US1   -25-

Serial No. 09/884,672
Art Unit No. 2134

38. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 21.

39. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 22.

40. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 23.

Serial No. 09/884,672
Art Unit No. 2134

41. (original) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing ad-hoc radio communication, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 24.

42. (canceled)

43. (canceled)

JP920000134US1   -27-